UNITED STATES DISTRICT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

CHRISTOPHER LAMIE, on behalf of himself and all others similarly situated, Plaintiff, v. LENDINGTREE, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Christopher Lamie, through his attorneys, brings this Class Action Complaint against the Defendant, LendingTree, LLC ("LendingTree" or "Defendant"), alleging as follows:

INTRODUCTION

1. LendingTree—a publicly traded lending service provider that aggregates loan leads from across the country—lost control over individuals' highly sensitive personal information in a data breach by cybercriminals ("Data Breach").

2. In February 2022, hackers exploited a "code vulnerability" in LendingTree's system which allowed them to bypass LendingTree's security and access information it stores on consumers.

3. Those consumers include Plaintiff, even though he has never used LendingTree's services in any way and has not applied for loans through LendingTree. Even so, LendingTree was in possession of Plaintiff's and other consumers' Social Security numbers, dates of birth, and home addresses, which were accessed in the Data Breach.

4. Plaintiff is part of over 200,000 other consumers whose information LendingTree compromised by employing inadequate data security protocols. Indeed, this is at least the third data breach LendingTree has suffered, with LendingTree failing to discover this most recent breach until June 2022, or *four months* after the hack.

5. What's more, hackers have posted the information on the dark web, bragging about the information they stole on every-day consumers.

6. When LendingTree finally disclosed the Data Breach in June 2022, it did not tell consumers that their information was on the dark web or disclose all the information that LendingTree lost in the breach.

7. In fact, LendingTree's breach notice downplayed the breach, telling consumers that it lost control over only consumers' Social Security numbers, dates of birth, and home addresses. But third-party researchers have confirmed that LendingTree is misrepresenting the breach's scope, as hackers have posted consumers' phone numbers, IP addresses, loan form submissions, loan types, and credit profile scores online for anyone to download.

8. LendingTree's misconduct violates state and federal law, industry standard practices, and its own internal policies.

9. Indeed, LendingTree is well-aware it has a duty to employ reasonable cybersecurity policies, telling consumers that it "maintain[s] physical, electronic, and procedural measures designed to safeguard your information from unauthorized access and disclosure."[1]

10. And LendingTree knows that failing to provide adequate cybersecurity leads to legal liability, disclosing to the Security and Exchange Commission ("SEC"): "The occurrence of any actual or attempted breach, failure of security or fraudulent activity, the reporting of such

[1] *See* LendingTree's Privacy Policy, https://www.lendingtree.com/legal/privacy-policy/ (Last visited July 6, 2022).

an incident, whether accurate or not, or our failure to make adequate or timely disclosures to the public or law enforcement agencies following any such event, whether due to delayed discovery or a failure to follow existing protocols, could result in claims made against us[…] which could result in state and/or federal litigation and related financial liabilities, as well as criminal penalties or civil liabilities[…] litigation and claims against us by consumers or third parties and related indemnification obligations."[2]

11. Plaintiff is a Data Breach victim whose highly sensitive information was compromised in the Data Breach. In the four-month span between when the Data Breach started and LendingTree disclosed it, Plaintiff suffered repeated identity theft, including fraudulent account openings, unwanted address changes, and fraudulent charges. Because LendingTree had not disclosed the Data Breach immediately after it happened, Plaintiff could not proactively protect himself from this identity theft, nor could he understand why it was happening.

12. As a result, Plaintiff brings this Class Action on behalf of himself and all others harmed by LendingTree's misconduct.

PARTIES

13. Plaintiff, is a natural person and citizen of Massachusetts, residing in Watertown, Massachusetts, where he intends to remain. Plaintiff is a Data Breach victim with no prior relationship with LendingTree. Even so, he received LendingTree's Breach Notice in June 2022.

14. Defendant, LendingTree, is a Delaware Limited Liability Company with its principal place of business in North Carolina at 1415 Vantage Park Drive, Suite 700, Charlotte, North Carolina 28203. LendingTree's sole "Manager" is Douglas R. Lebda, who is a citizen of North Carolina.

[2] *See* LendingTree's 2021 Annual Report at https://sec.report/Document/0001434621-22-000009/#i1edd2cf7c4fc4604b5c29461b3ac2691_19 (last visited July 6, 2022).

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, does substantial business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in this District.

17. Venue is proper under 18 U.S.C § 1391(b)(1) because LendingTree's principal place of business is in this District.

BACKGROUND FACTS

a. LendingTree's Business

18. LendingTree is a lending service provider advertising itself as a "marketplace" for mortgages and "various financial borrowing needs including auto loans, small business loans, personal loans, credit cards, and more."[3]

19. To conduct its business, LendingTree collects highly sensitive personal information on consumers, including their "personally identifiable information" ("PII"). In fact, LendingTree discloses that it collects PII on consumers through three sources:

[3] *See* LendingTree's "About" page on its website, https://www.lendingtree.com/press/ (last visited July 6, 2022).

How We Collect Information

1. Information provided by you: We collect information from you when you enter it or otherwise provide it in connection with an inquiry into our Services. This information could be provided via an online form, over the phone, or via other means in which you interact with our Services.

2. Information from third parties: Information is collected from credit bureaus, lead generators and other partners who may have data on your financial profile, home, or other demographic information.

3. Information from cookies and other tracking technologies: We use cookies, web beacons, and similar technologies to record your preferences, track the use of our Site and collect information. This information may include internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data. We may combine this automatically collected log information with other information we collect about you. You may choose to set your web browser to refuse cookies, or to alert you when cookies are being sent. If you do so, please note that some parts of our Sites may not function properly.

20. In other words, LendingTree not only collects information directly from consumers, but also indirectly from consumers who have no prior relationship with LendingTree.

21. In collecting and storing this highly sensitive PII, LendingTree knows it has a duty to protect it. Indeed, its Privacy Policy states that LendingTree "maintain[s] physical, electronic, and procedural measures designed to safeguard your information from unauthorized access and disclosure."[4]

22. And as a publicly traded company, LendingTree also discloses that it knows the risk that data breaches pose to its business and that hackers target sensitive information like PII: "In the processing of consumer transactions, our businesses collect, use, store, disclose, transfer, and otherwise process a large volume of personal information and other confidential, proprietary and sensitive data. Breaches or failures of security involving our systems or website[…] have occurred in the past and may occur in the future, and have in the past resulted in, and could in the future result in, the theft, unauthorized access, acquisition, use, disclosure, modification or

[4] *See* LendingTree's Privacy Policy, https://www.lendingtree.com/legal/privacy-policy/ (Last visited July 6, 2022).

misappropriation of personal information of our consumers[.]"[5]

23. As a result, LendingTree understands that a "failure of our data security processes" could lead to civil liability: "The occurrence of any actual or attempted breach, failure of security or fraudulent activity, the reporting of such an incident, whether accurate or not, or our failure to make adequate or timely disclosures to the public or law enforcement agencies following any such event, whether due to delayed discovery or a failure to follow existing protocols, could result in claims made against us[…] which could result in state and/or federal litigation and related financial liabilities[…] litigation and claims against us by consumers[.]"[6]

b. LendingTree's Prior Data Breaches

24. Despite understanding its duty to safeguard the PII it collects, LendingTree has a sordid history with data security.

25. Indeed, the company has been hacked at least two times before the Data Breach.

26. In 2008, LendingTree's own employees stole consumer data from LendingTree's internal systems in an act of corporate espionage, transferring it to LendingTree's competitors.[7] The breach led consumers to sue LendingTree over its inadequate data security policies.

27. And again, in January 2022, LendingTree disclosed another data breach affecting an unknown number of consumers.[8]

28. In each case, LendingTree was unable to prevent, detect, or stop the breaches

[5] *See* LendingTree's 2021 Annual Report at https://sec.report/Document/0001434621-22-000009/#i1edd2cf7c4fc4604b5c29461b3ac2691_19 (last visited July 6, 2022).

[6] *Id.*

[7] *See* Data Breach Victims File Lawsuit Against LendingTree, CNN.com, https://www.crn.com/news/security/208200116/data-breach-victims-file-lawsuit-against-lendingtree.htm?itc=refresh (last visited July 6, 2022).

[8] *See* Breach Notice Letter to the Massachusetts Office of Consumer Affairs and Business Regulation, https://www.mass.gov/doc/assigned-data-beach-number-25815-lendingtree-llc/download (last visited July 6, 2022).

from happening before cybercriminals accessed and stole consumer PII, meaning it has been unwilling or unable to implement reasonable cybersecurity.

c. The February 2022 Data Breach

29. As explained above, LendingTree collects PII on consumers from across the country using several means.

30. LendingTree collects and maintains that PII in its computer systems.

31. In collecting and maintaining the PII, LendingTree has a duty to safeguard the data according to its internal policies and state and federal law.

32. According to LendingTree, in February 2022, hackers exploited a "code vulnerability" in LendingTree's systems, allowing them to access the PII belonging to over 200,000 consumers.[9]

33. But LendingTree did not immediately detect the Data Breach, nor would it for another four months.

34. In that time, Plaintiff suffered at least four instances of identity theft, as further described below.

35. In June 2022, LendingTree finally discovered the Data Breach and began notifying consumers with a breach notice ("Breach Notice").

36. But the Breach Notice obfuscated the Data Breach's nature and downplayed its harm. Indeed, the Breach Notice said that LendingTree had lost control over only consumers' "social security number[s], date[s] of birth, and street address[es]."

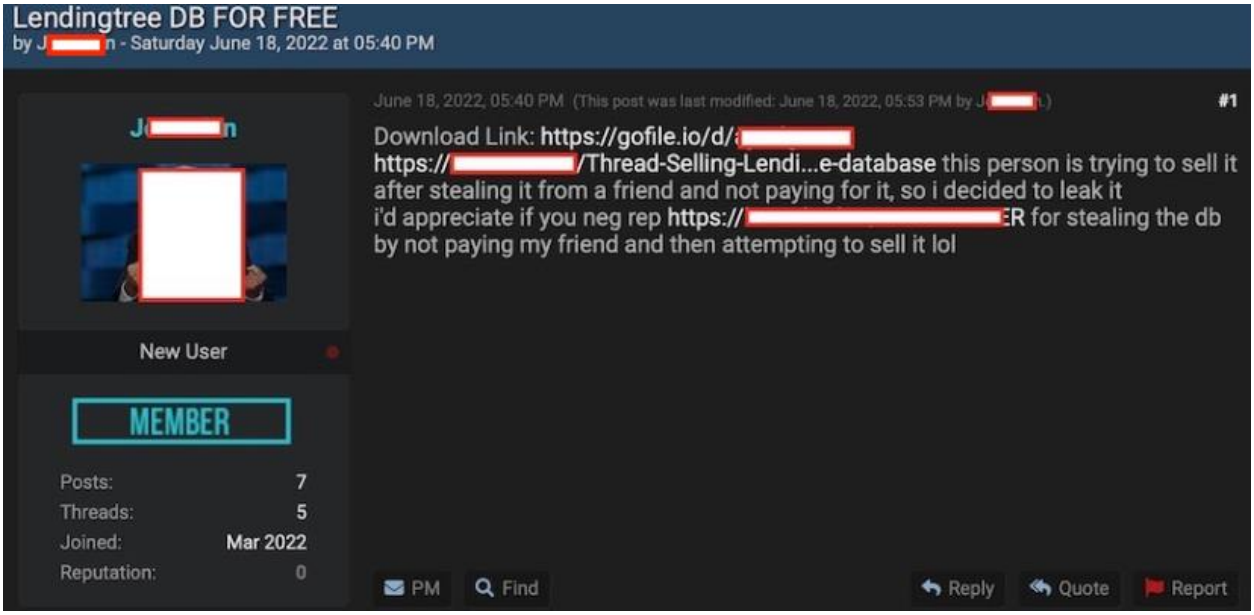
37. But third-party investigation would prove that false.

38. Before LendingTree even notified consumers about the breach, hackers were

[9] *See* LendingTree's Breach Notice, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-363.pdf (last visited July 6, 2022). A copy of LendingTree's Breach Notice is attached as **Exhibit A**.

advertising consumers' PII online.[10]

39. In fact, a third-party publication, Restore Privacy, found that hackers had posted consumer PII on the dark web in June 2022, where "two different forum users posted the database allegedly breached from LendingTree.com. In the most recent post, dated June 18, 2022, the user decided to post the 'LendingTree DB for free'[,]" then including a screenshot of the hackers' post:[11]



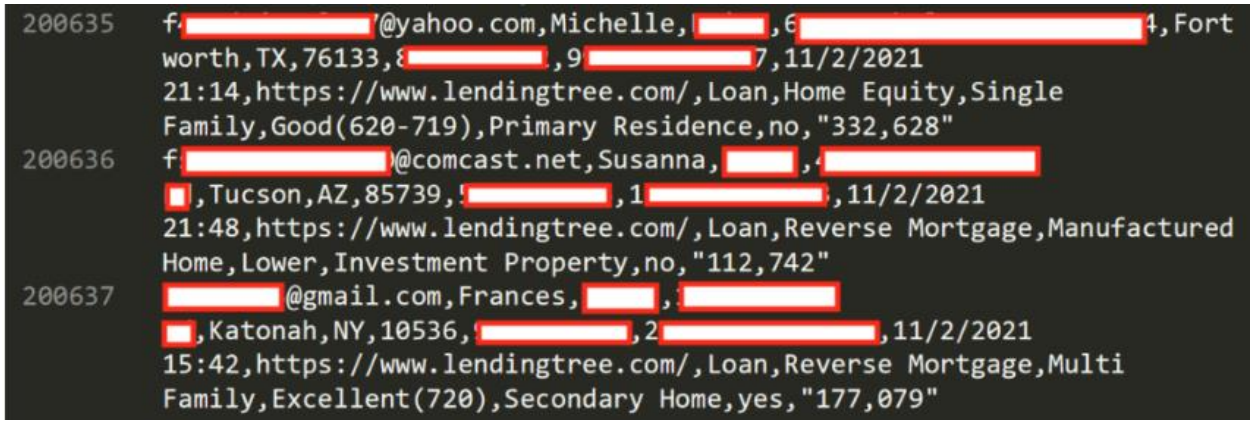
40. Investigators at Restore Privacy downloaded the information and confirmed that the data included PII belonging to real people: "**All of the entries** that we attempted to verify using publicly available search tools **match real-world people**." (emphasis in original).[12]

41. In fact, the stolen data included information clearly depicting it as stolen from LendingTree's website:

[10] *See* Hacker Leaks Database Claiming to be from LendingTree, RestorePrivacy.com, https://restoreprivacy.com/lendingtree-data-breach-2022/#comments (last visited July 6, 2022).

[11] *Id.*

[12] *Id.*



13

42. What's more, the investigation revealed that the Data Breach exposed much more information than LendingTree's Breach Notice disclosed to consumers, as the dark web post had consumers' emails, full names, physical addresses, phone numbers, IP addresses, loan submission dates, lead source, loan type, home description, credit score, property use, military status, and price.[14]

43. In other words, the breach involved highly sensitive PII that criminals can use to steal individuals' identities, available for anyone to download and exploit. As Restore Privacy put it, "Not only does this put all of these people at risk for identity theft and financial fraud, it also puts them at risk for targeted attacks pertaining to home loans. Cyber criminals could utilize the private information of these applications, including names, addresses, phone numbers, and credit scores, to open accounts in the victim's name and possibly carry out financial transactions."[15]

44. On information and belief, LendingTree caused the Data Breach to happen

[13] *Id.*

[14] *Id.*

[15] *Id.*

because it failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, after which it lost control over consumers' PII. LendingTree's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII, even after LendingTree had experience *two* prior data breaches. Further, the Breach Notice makes clear that LendingTree cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

d. Plaintiff's Experience

45. Plaintiff is a Data Breach victim, receiving LendingTree's Breach Notice in July 2022. He also contacted LendingTree by phone to confirm he was part of the breach and received confirmation from LendingTree's representatives.

46. Plaintiff has no prior relationship with LendingTree and he does not know how the company accessed or collected his data. Indeed, Plaintiff has never applied for a loan through LendingTree, nor given the company permission to use or access his PII.

47. After the Data Breach happened, but before LendingTree disclosed it, Plaintiff suffered at least four instances of identity theft. In April 2022, Plaintiff suffered fraudulent charges on his personal credit card. In May 2022, someone attempted to open an account in his name with an online store, someone else changed his USPS home address, and another person tried to open financial accounts in his name with three different institutions.

48. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This

goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

e. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

49. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

50. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the

appropriate measures to protect the PII in their possession.

51. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

52. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

53. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

54. One such example of criminals using PII for profit is the development of "Fullz" packages.

55. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

56. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the

proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

57. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

58. Defendant's failure to properly detect the Data Breach and notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

f. LendingTree failed to adhere to FTC guidelines.

59. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as LendingTree, should employ to protect against the unlawful exposure of PII.

60. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

61. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

62. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. LendingTree's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

65. Plaintiff sues on behalf of himself and the proposed Class under Rule 23(b)(2) and 23(b)(3), defined as follows:

> All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Defendant in June 2022.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

66. Plaintiff reserves the right to amend the class definition.

67. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of over 200,000 members for the Class, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class's interests and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

v. Whether Defendant's Breach Notice was reasonable;

vi. Whether the Data Breach caused Plaintiff and the Class injuries;

vii. What the proper damages measure is; and

viii. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

68. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

69. Plaintiff realleges all previous paragraphs as if fully set forth below.

70. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at

unauthorized access.

71. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

72. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

73. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and members of the Class's personal information and PII.

74. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that

unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

75. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class's PII and the importance of exercising reasonable care in handling it.

76. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

77. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se

(On Behalf of Plaintiff and the Class)

78. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

79. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

80. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

81. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect consumers' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers in the event of a breach, which ultimately came to pass.

82. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

83. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

84. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

85. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

86. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

87. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

88. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

89. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment

(On Behalf of Plaintiff and the Class)

90. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

91. Defendant received a benefit from Plaintiff and the Class by obtaining their PII.

92. Defendant appreciated or had knowledge of the benefits conferred upon itself. Defendant also benefited from the receipt of Plaintiff and members of the Class's PII, as this was used to conduct its business.

93. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant failed to adequately protect their PII.

94. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT IV
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

95. Plaintiff incorporates all previous paragraphs as if fully set forth below.

96. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

97. Defendant owed a duty to the individuals it obtained information from, including Plaintiff and the Class, to keep this information confidential.

98. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff and the Class's PII is highly offensive to a reasonable person.

99. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

100. The Data Breach constitutes an intentional interference with Plaintiff and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

101. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

102. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

103. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

104. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available to disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

105. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since those records are still maintained by Defendant with their inadequate cybersecurity system and policies.

106. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the records of Plaintiff and the

Class. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Class)

107. Plaintiff incorporates all previous paragraphs as if fully set forth below.

108. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein.

109. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

110. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

111. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect Plaintiff's and the Class's data.

112. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

113. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

114. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 11th day of July, 2022.

Respectfully Submitted,

By: */s/ Joel R. Rhine*

Joel R. Rhine
NCSB # 16028
Martin A. Ramey
NCSB # 33617
RHINE LAW FIRM, PC
1612 Military Cutoff Road, Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
Fax: (910) 772-9062
jrr@rhinelawfirm.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

*Pro hac vice pending

Attorneys for Plaintiff